kod szkolenia: ECIH / PL AA 3d

Certified Incident Handler

Autoryzowane szkolenie EC-Council – ECIH v2 - EC-Council Certified Incident Handler

Realizowane jest w formie wykładu oraz praktycznych warsztatów.

Szkolenie EC-Council Certified Incident Handler v2 (E|CIH) to kompleksowy program na poziomie specjalistycznym, który przekazuje wiedzę i umiejętności potrzebne organizacjom do skutecznego radzenia sobie z incydentami związanymi z bezpieczeństwem informatycznym. Kurs omawia podstawowe zasady i techniki wykrywania i reagowania na obecne i nowo pojawiające się zagrożenia bezpieczeństwa komputerowego. Po ukończeniu szkolenia kursanci będą mieli okazję zapisać się na egzamin ECIH. Certyfikat ECIH jest wysoko oceniany i pomaga zwiększyć szanse zatrudnienia na stanowiskach specjalistów ds. cyberbezpieczeństwa na całym świecie.

Przeznaczenie szkolenia

Szkolenie skierowane jest do:

- administratorów sieci
- osób odpowiedzialnych za infrastrukturę informatyczną
- inżynierów systemowych
- audytorów VA (Vulnerability Assessment)
- osób zarządzających ryzykiem od strony IT
- inżynierów bezpieczeństwa
- analityków bezpieczeństwa
- specjalistów CFI (Cyber Forensic Investigators)
- pracowników SOC

- pracowników IT planujących podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji

Dla osób nie będących specjalistami z zakresu bezpieczeństwa IT szkolenie może być zbyt intensywne ale pozwoli zwiększyć świadomość dotyczącą obsługi zdarzeń i właściwego reagowania na zagrożenia. Specjaliści ds. bezpieczeństwa informatycznego, audytorzy i analitycy bezpieczeństwa oraz pentesterzy będą mogli ugruntować, usystematyzować bądź uzupełnić swoją wiedzę.

Korzyści wynikające z ukończenia szkolenia

Organizacje są celem nieustannych ataków a dzięki wiedzy i umiejętnościom zdobytym na kursie E|CIH, eksperci będą mogli nie tylko wykrywać incydenty, lecz także błyskawicznie nimi zarządzać, jak i całościowo na nie odpowiadać. Program szkoleniowy uczy biegłej obsługi i reakcji na takie zdarzenia jak naruszenia bezpieczeństwa sieci, infekcje złośliwym oprogramowaniem czy zagrożenia związane z atakami wewnętrznymi. Ponadto studenci poznają podstawy informatyki śledczej, jej rolę w obsłudze zdarzeń i reagowaniu na nie. Kurs omawia również pracę zespołów zarzadzania i reagowania na incydenty oraz przedstawia techniki stosowane przy przywracaniu działania firmy. Kursanci dowiedzą się, jak radzić sobie w sytuacjach naruszenia bezpieczeństwa, poznają metody oceny ryzyka oraz różne przepisy związane z obsługą incydentów. Po ukończeniu tego kursu uczestnicy będą mogli tworzyć spójne i przemyślane zasady obsługi zdarzeń.

Uczestnicy szkolenia zrozumieją procesy obsługi i reagowania na incydenty i nauczą się :

- stosować procedury pierwszej reakcji i przygotowywać „grunt” dla informatyki śledczej
- obsługiwać incydenty i adekwatnie reagować
- obsługiwać zdarzenia związane ze złośliwym oprogramowaniem
- reagować na incydenty związane z bezpieczeństwem poczty e-mail, aplikacji internetowych
- obsługiwać i reagować na naruszenia bezpieczeństwa sieci
- radzić sobie z różnymi z incydentami związanymi z bezpieczeństwem chmury
- wykrywać i reagować na zagrożenia wewnętrzne

Metoda egzaminowania

Uwaga: Jeśli uczestnik chciałby zdawać egzamin ECIH w formule online (z dowolnego miejsca) z tzw. ochroną zdalną, obowiązuje dodatkowa opłata 100 USD netto. Koszt obejmuje wynajęcie osoby nadzorującej egzamin (tzw. proktora). Zakupu dokonujemy indywidulanie na stronie vendora: https://store.eccouncil.org/product/voucher-upgrade-rps-to-vue/

Opis egzaminu

- Tytuł egzaminu: EC-Council Certified Incident Handler
- Liczba pytań: 100
- Czas trwania: 3 godziny
- Format: pytania wielokrotnego wyboru

Oczekiwane przygotowanie słuchaczy

Wymagana dobra znajomość systemów operacyjnych Windows oraz Linux, wiedza o protokołach i usługach sieciowych. Zalecane przynajmniej dwuletnie doświadczenie w cyberbezpieczeństwie.

Język szkolenia

- Szkolenie: polski
- Materiały: angielski

Czas trwania

3 dni / 21 godzin

Agenda szkolenia

1. Wprowadzenie do obsługi i reagowania na incydenty

- Przegląd koncepcji bezpieczeństwa informacji
- Zrozumienie zagrożeń bezpieczeństwa informacji i wektorów ataków
- Zrozumienie incydentów związanych z bezpieczeństwem informacji
- Przegląd zarządzania incydentami
- Przegląd zarządzania podatnościami
- Przegląd oceny zagrożeń
- Koncepcje zarządzania ryzykiem
- Koncepcje automatyzacji i orkiestracji reagowania na incydenty

- Najlepsze praktyki w zakresie obsługi incydentów i reagowania
- Przegląd standardów
- Przegląd ram cyberbezpieczeństwa
- Znaczenie przepisów w obsłudze incydentów
- Obsługa incydentów i zgodność z prawem

2. Proces obsługi i reagowania na incydenty

- Przegląd procesu obsługi i reagowania na incydenty (IH&R)
- Przygotowanie do obsługi incydentów i reagowania
- Rejestrowanie i przypisywanie incydentów
- Segregacja incydentów
- Notyfikacja
- Powstrzymywanie
- Zbieranie dowodów i analiza kryminalistyczna
- Likwidacja szkód
- Przywracanie
- Działania po zdarzeniach

3. Gotowość do działań kryminalistycznych i pierwsza odpowiedź

- Wprowadzenie do informatyki śledczej
- Przegląd gotowości kryminalistycznej
- Przegląd pierwszej odpowiedzi
- Przegląd dowodów cyfrowych
- Zrozumienie zasad gromadzenia dowodów cyfrowych
- Zbieranie dowodów
- Zabezpieczanie dowodów
- Akwizycja danych
- Kolekcjonowanie ulotnych dowodów
- Gromadzenie dowodów statycznych
- Analiza dowodów
- Przegląd anty-kryminalistycznych technik

4. Obsługa i reagowanie na incydenty związane ze złośliwym oprogramowaniem

- Omówienie reakcji na incydenty związane ze złośliwym oprogramowaniem
- Przygotowanie do obsługi incydentów związanych ze złośliwym oprogramowaniem
- Wykrywanie incydentów związanych ze złośliwym oprogramowaniem
- Powstrzymywanie incydentów związanych ze złośliwym oprogramowaniem
- Eliminacja incydentów związanych ze złośliwym oprogramowaniem
- Odzyskiwanie po incydentach związanych ze złośliwym oprogramowaniem
- Wytyczne dotyczące zapobiegania incydentom związanym ze złośliwym oprogramowaniem

5. Obsługa i reagowanie na incydenty związane z bezpieczeństwem poczty e-mail

- Przegląd incydentów związanych z bezpieczeństwem poczty e-mail
- Przygotowanie do obsługi incydentów związanych z bezpieczeństwem poczty e-mail
- Wykrywanie i powstrzymywanie incydentów związanych z bezpieczeństwem poczty e-mail

- Eliminacja incydentów związanych z bezpieczeństwem poczty e-mail
- Odzyskiwanie po incydentach związanych z bezpieczeństwem poczty e-mail

6. Obsługa i reagowanie na incydenty związane z bezpieczeństwem sieci
- Przegląd incydentów związanych z bezpieczeństwem sieci
- Przygotowanie do obsługi incydentów związanych z bezpieczeństwem sieci
- Wykrywanie i walidacja incydentów związanych z bezpieczeństwem sieci
- Postępowanie w przypadku nieautoryzowanych incydentów dostępu
- Postępowanie w przypadku incydentów niewłaściwego użytkowania
- Obsługa incydentów odmowy usługi (DoS)
- Obsługa incydentów związanych z bezpieczeństwem sieci bezprzewodowych

7. Obsługa i reagowanie na incydenty związane z bezpieczeństwem aplikacji internetowych
- Przegląd obsługi incydentów aplikacji internetowych
- Zagrożenia i ataki na bezpieczeństwo aplikacji internetowych
- Przygotowanie do obsługi incydentów związanych z bezpieczeństwem aplikacji internetowych
- Wykrywanie i analiza incydentów związanych z bezpieczeństwem aplikacji internetowych
- Powstrzymywanie incydentów związanych z bezpieczeństwem aplikacji internetowych
- Eliminacja incydentów związanych z bezpieczeństwem aplikacji internetowych
- Odzyskiwanie po incydentach związanych z bezpieczeństwem aplikacji internetowych
- Najlepsze praktyki zabezpieczania aplikacji internetowych

8. Obsługa i reagowanie na incydenty związane z bezpieczeństwem w chmurze
- Koncepcje przetwarzania w chmurze obliczeniowej
- Przegląd obsługi incydentów związanych z bezpieczeństwem w chmurze
- Zagrożenia i ataki w zakresie bezpieczeństwa chmury
- Przygotowanie do obsługi incydentów związanych z bezpieczeństwem w chmurze
- Wykrywanie i analiza incydentów związanych z bezpieczeństwem w chmurze
- Ograniczanie incydentów związanych z bezpieczeństwem w chmurze
- Eliminacja incydentów związanych z bezpieczeństwem w chmurze
- Odzyskiwanie po incydentach związanych z bezpieczeństwem w chmurze
- Najlepsze praktyki dotyczące incydentów w chmurze

9. Postępowanie i reagowanie na zagrożenia wewnętrzne
- Wprowadzenie do zagrożeń wewnętrznych
- Przygotowanie do radzenia sobie z zagrożeniami wewnętrznymi
- Wykrywanie i analiza zagrożeń wewnętrznych
- Powstrzymywanie zagrożeń wewnętrznych
- Eliminacja zagrożeń wewnętrznych
- Odzyskiwanie po atakach wewnętrznych
- Najlepsze praktyki w walce z zagrożeniami wewnętrznymi